Chapter 6
Integration of Security in the Development Lifecycle of Dependable Automotive CPS

Georg Macher
AVL List GmbH, Austria

Eric Armengaud
AVL List GmbH, Austria

Christian Kreiner
Graz University of Technology, Austria

Eugen Brenner
Graz University of Technology, Austria

Christoph Schmittner
Austrian Institute of Technology, Austria

Zhendong Ma
Austrian Institute of Technology, Austria

Helmut Martin
Virtual Vehicle Research Center, Austria

Martin Krammer
Virtual Vehicle Research Center, Austria

ABSTRACT

The exciting new features, such as advanced driver assistance systems, fleet management systems, and autonomous driving, drive the need for built-in security solutions and architectural designs to mitigate emerging security threats. Thus, cybersecurity joins reliability and safety as a cornerstone for success in the automotive industry. As vehicle providers gear up for cybersecurity challenges, they can capitalize on experiences from many other domains, but nevertheless must face several unique challenges. Therefore, this article focuses on the enhancement of state-of-the-art development lifecycle for automotive cyber-physical systems toward the integration of security, safety and reliability engineering methods. Especially, four engineering approaches (HARA at concept level, FMEA and FTA at design level and HSI at implementation level) are extended to integrate security considerations into the development lifecycle.

DOI: 10.4018/978-1-7998-7705-9.ch006

INTRODUCTION

Before the introduction of wireless connections and automated driving functionalities, vehicles were physically isolated machines with mechanical controls. Extra-functional properties of concern were mainly timing, reliability and functional safety. The emergence of cyber-physical automotive systems over the last decades has affected the development of vehicles, promising to improve the safety of drivers and support new applications. The deployment of connected CPS especially is leading to a strong re-organization of the automotive market, moving from "vehicle as a product" to "transportation as a service". Hence, the availability of information (e.g., powertrain control strategy, traffic information, as well as infotainment and connectivity) is shifting the customer added value of the passenger car.

In this context, the rising vehicle-to-vehicle and vehicle-to-infrastructure connectivity causes multiple inter-vehicle connections as well as capabilities for (wireless) networking with other vehicles and non-vehicle entities. Automotive systems are developing from stand-alone systems towards systems of systems, interacting and coordinating with each other and influencing vehicle actions. Connections are not restricted to internal systems (e.g. steering, sensor, actuator, and communications) but also include other road users and the infrastructure. Current vehicles already utilize connectivity for over-the-air updates, smart maintenance, remote tracking or insurance services.

A well-known demonstration of security risks was the hack of a Jeep Cherokee (Miller & Valasek, Remote Exploitation of an Unaltered Passenger Vehicle, 2015). The intrusion started through a vulnerability in the cellular network configuration, progressed from the telematic system and ultimately affected even safety-critical control units. The Attackers were able to influence braking, steering and acceleration. A similar weakness was also found by the German automotive club ADAC in the ConnectedDrive system installed in BMW vehicles. A vulnerability in the communication configuration allowed an attacker to access the communication.

Audi and Corvette examples demonstrated that attacks are not always triggered by direct remote connectivity. The CrySyS Lab of the Budapest University of Technology and Economics demonstrated that an infected USB stick was sufficient to deactivate the Airbags in an Audi TT without giving either the rest of the system or the driver notice of the deactivation (Szijj, Buttyan, & Szalay, 2015).

In the case of the Corvette the attack was conducted through an insurance OBD-dongle. While the on-board diagnosis (OBD) interface is intended for maintenance and error reports, it also allows monitoring of the vehicle speed and location. The insurance company offered personalized insurance deals, based on driving behavior. The OBD dongle monitored speed and location and transmitted the data to the insurance company. Researchers were able to misuse the same connection to perform a proof-of-concept attack on the braking system of the vehicle.

After 2018, all vehicles sold in the EU, are required to be able to send GPS coordinates, impact sensor and airbag deployment information in the case of an accident. This so-called eCall functionality requires wireless connectivity. GM offers in North America already a similar service through the OnStar Network, which was successfully attacked (Baldwin, 2015).

While wireless connections open the attack surface, increased automated driving functionalities and data collection have introduced further valuable targets for attacker. Motivation for such attacks range from inflicting financial damage on a competitor (e.g., loss of image), loss of confidentiality or privacy with respect to driver (e.g., profile) or car manufacturer (e.g., sensitive vehicle information), or operational or safety impacts. Taking into account the fact that worldwide over a million people fall victim to cybercrime every day and that the global cost of cybercrime was assessed at 313 billion Euros in 2011